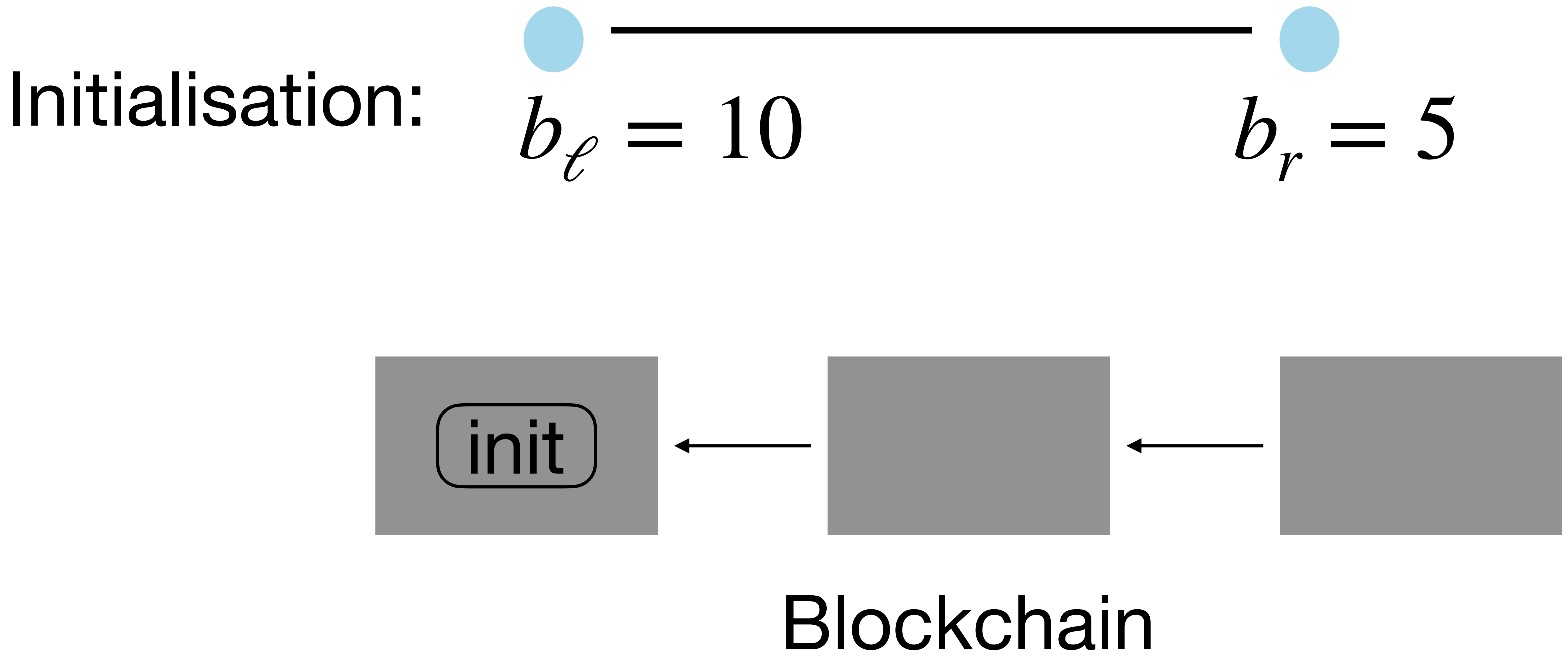
X-Transfer: Enabling and Optimising Cross-PCN Transactions

Lukas Aumayr, Zeta Avarikioti, Iosif Salem, Stefan Schmid, **Michelle Yeo**

NUS
National University
of Singapore

Payment channel networks

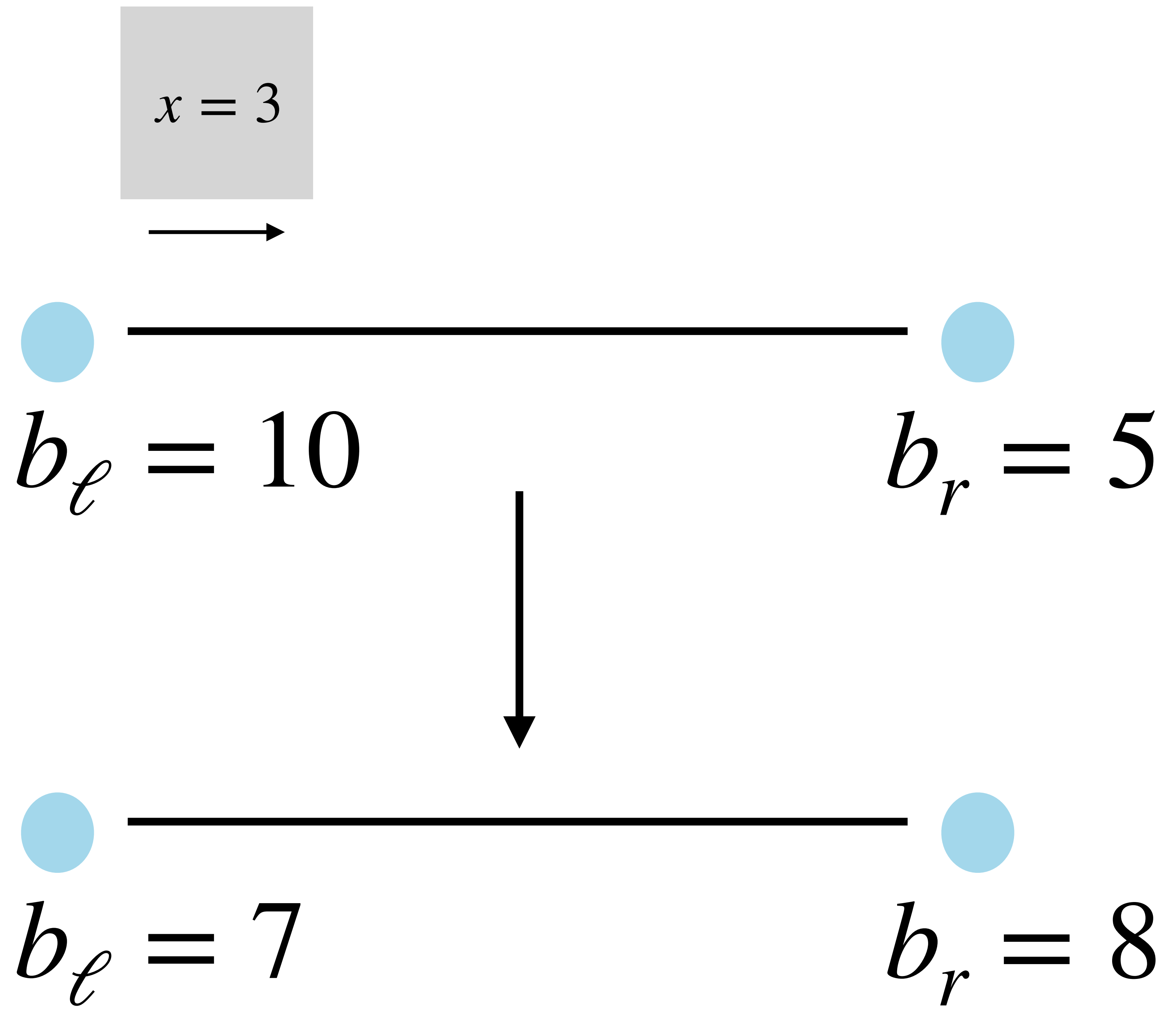
- Payment Channel Networks (PCNs) improve scalability and privacy of blockchains



Initialisation: $b_\ell = 10$ $b_r = 5$

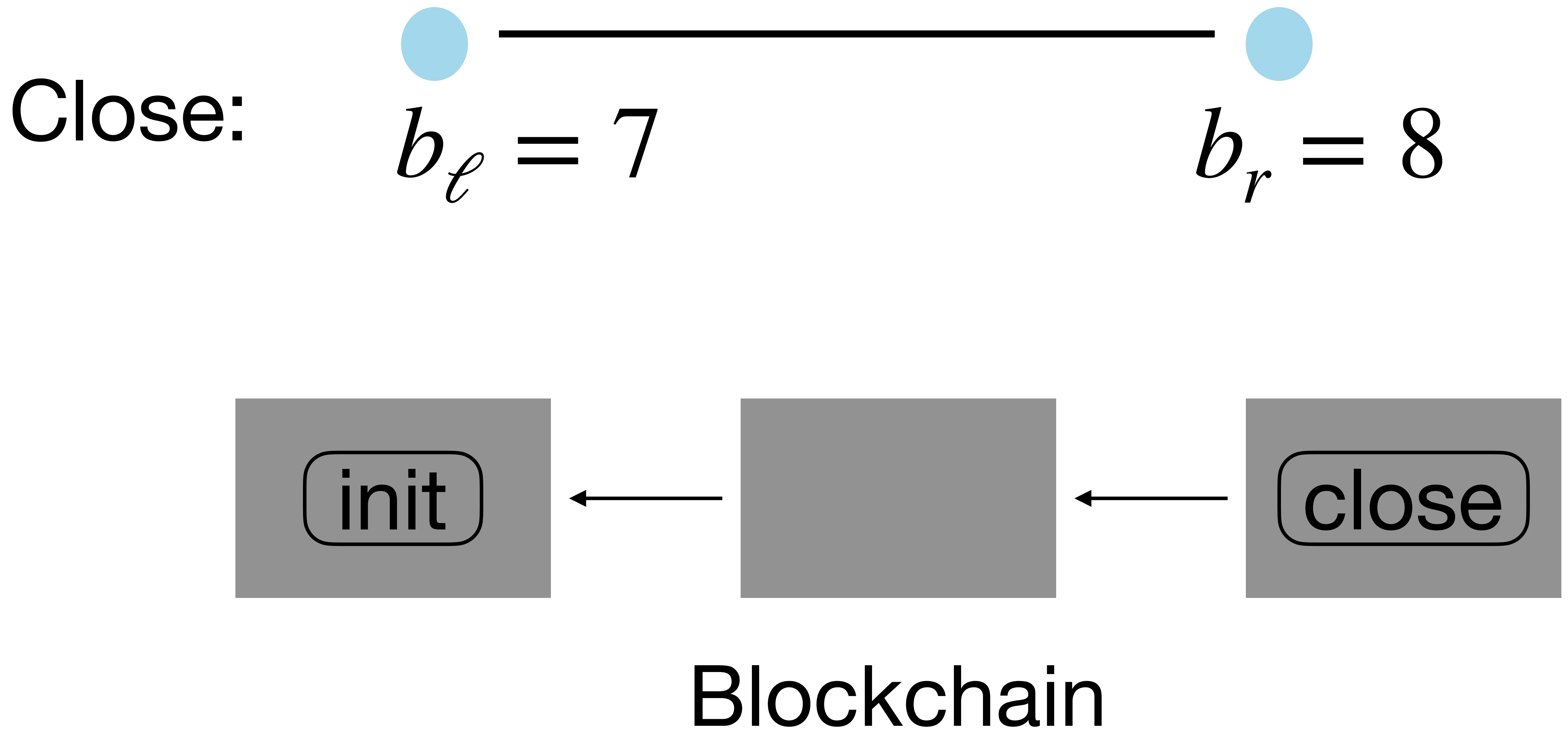
Payment channel networks

- Payment Channel Networks (PCNs) improve scalability and privacy of blockchains



Payment channel networks

- Payment Channel Networks (PCNs) improve scalability and privacy of blockchains



Close: $b_\ell = 7$ $b_r = 8$

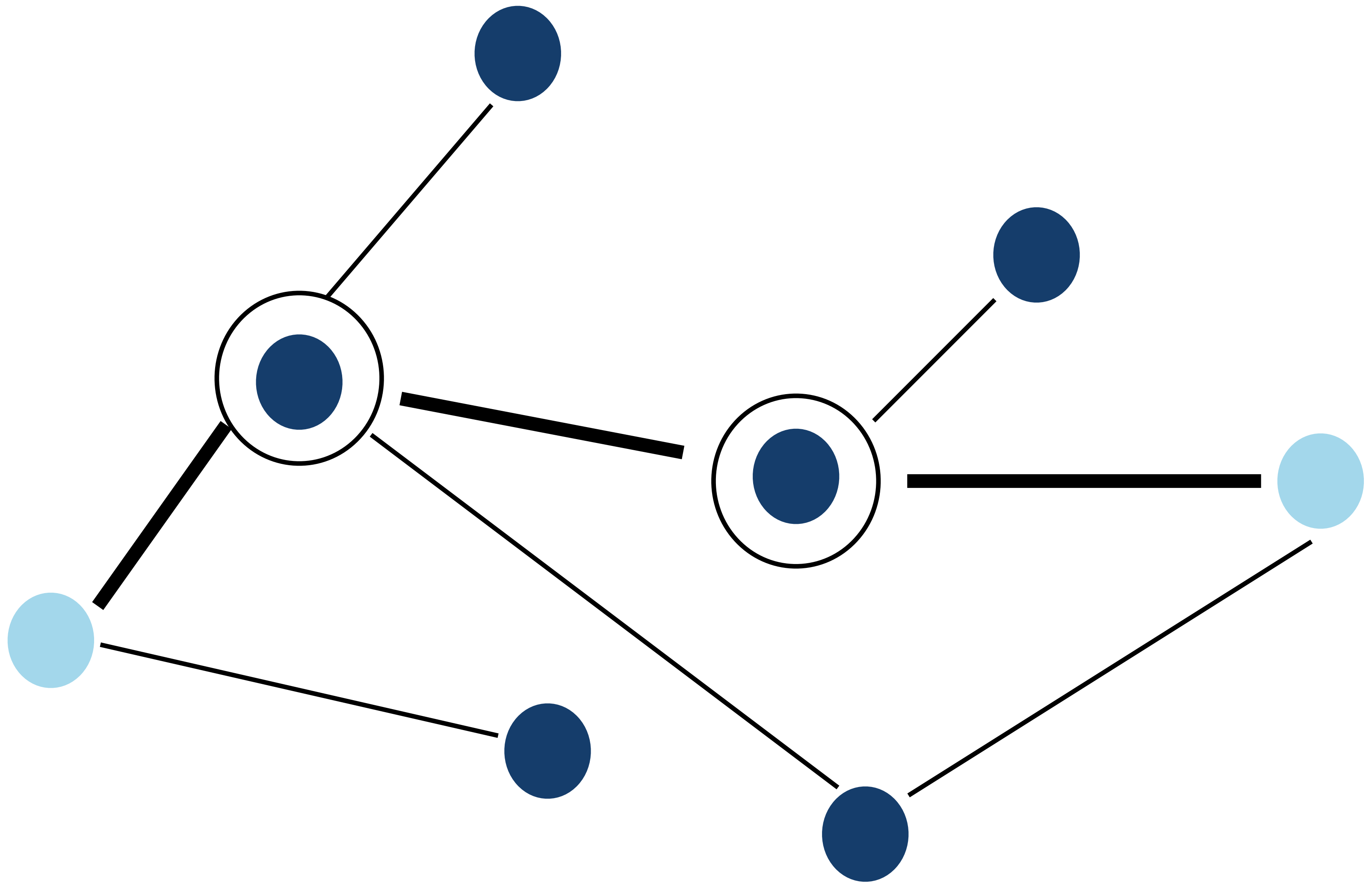
init

close

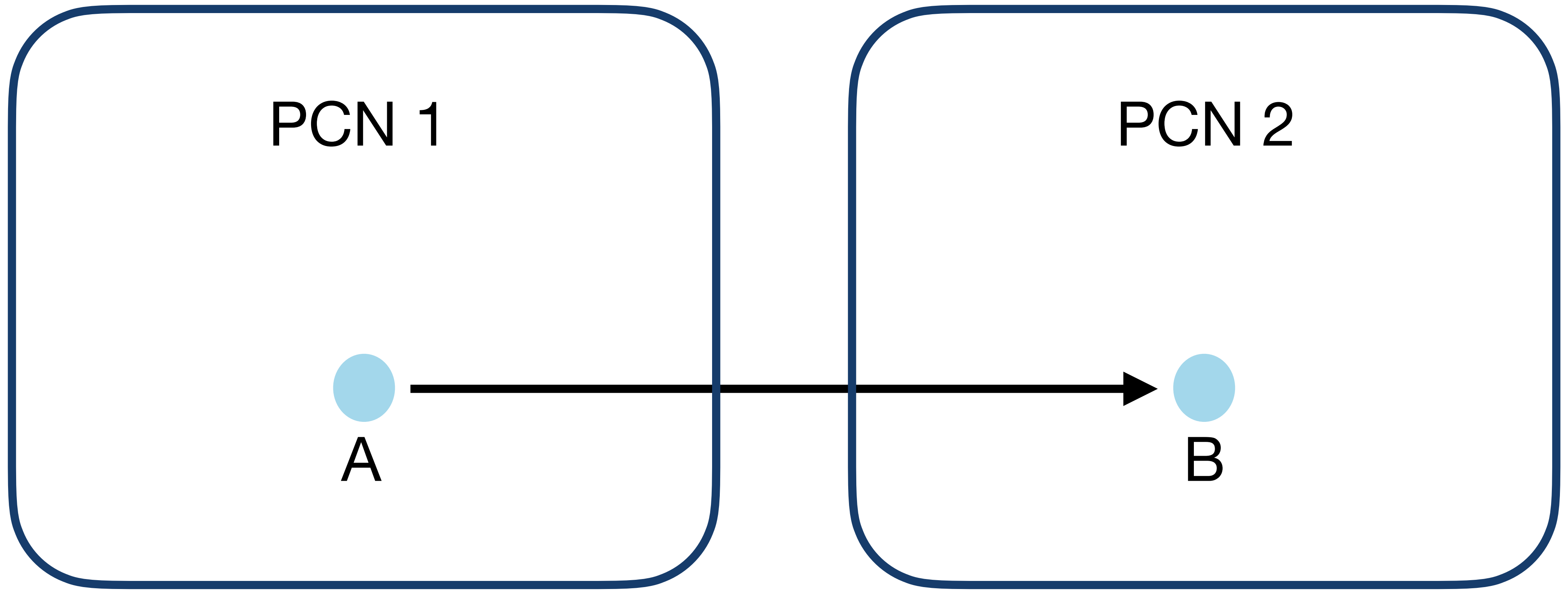
Blockchain

Payment channel networks

- Payment Channel Networks (PCNs) improve scalability of blockchains
- Intermediary nodes charge fees to forward payments



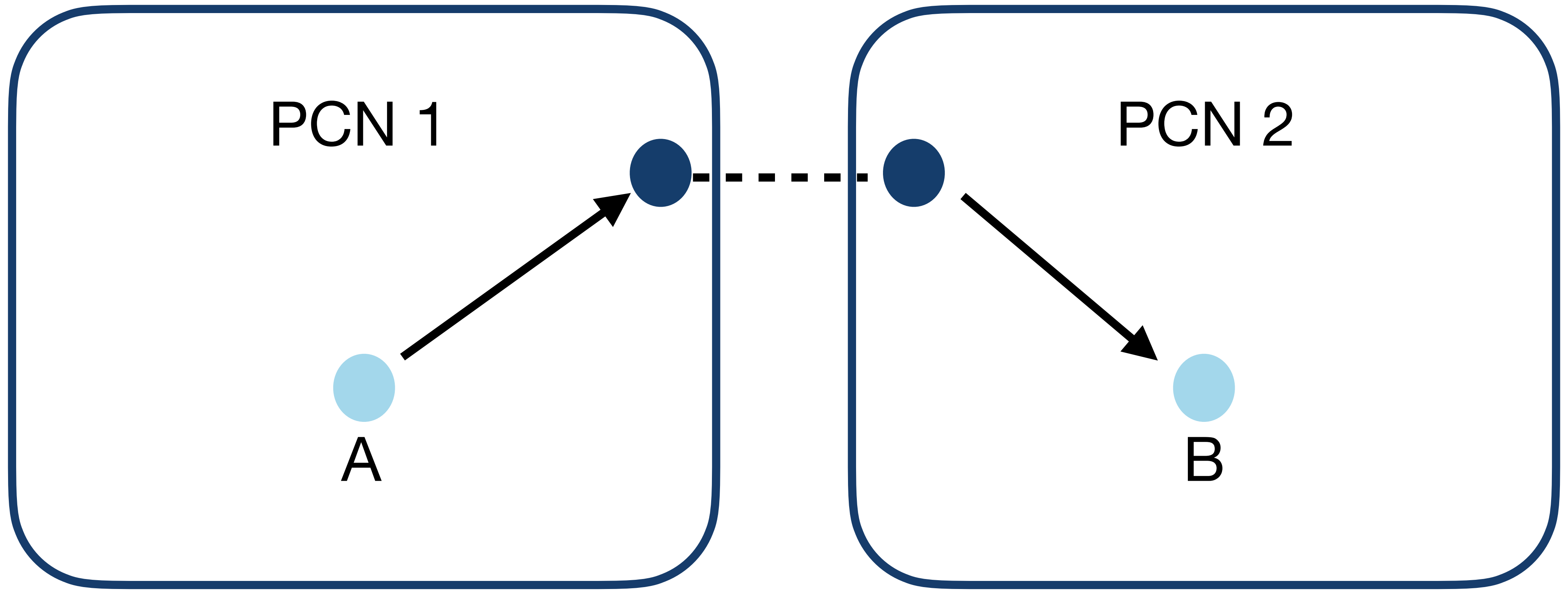
Secure and interoperable PCNs



Secure and interoperable PCNs

- Issues:

1. Interoperability: how to convert payments across two systems?

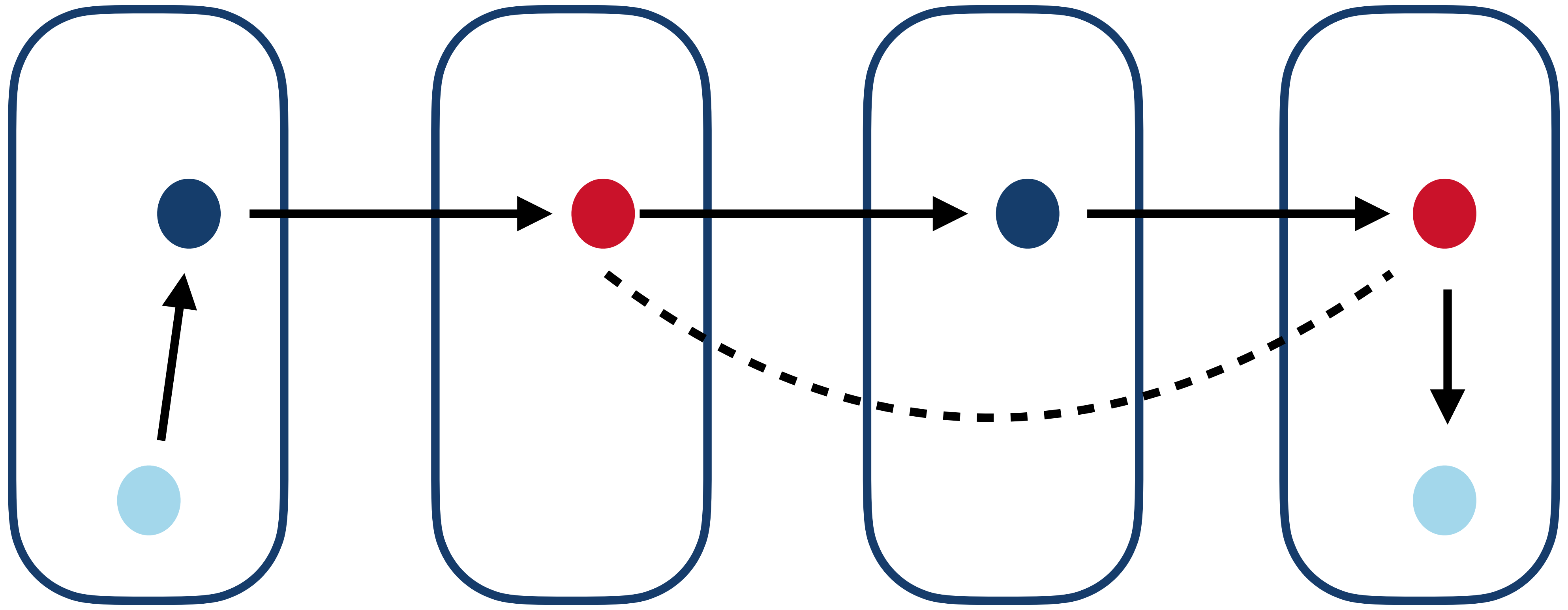


Secure and interoperable PCNs

- Issues:

1. Interoperability: how to convert payments across two systems?

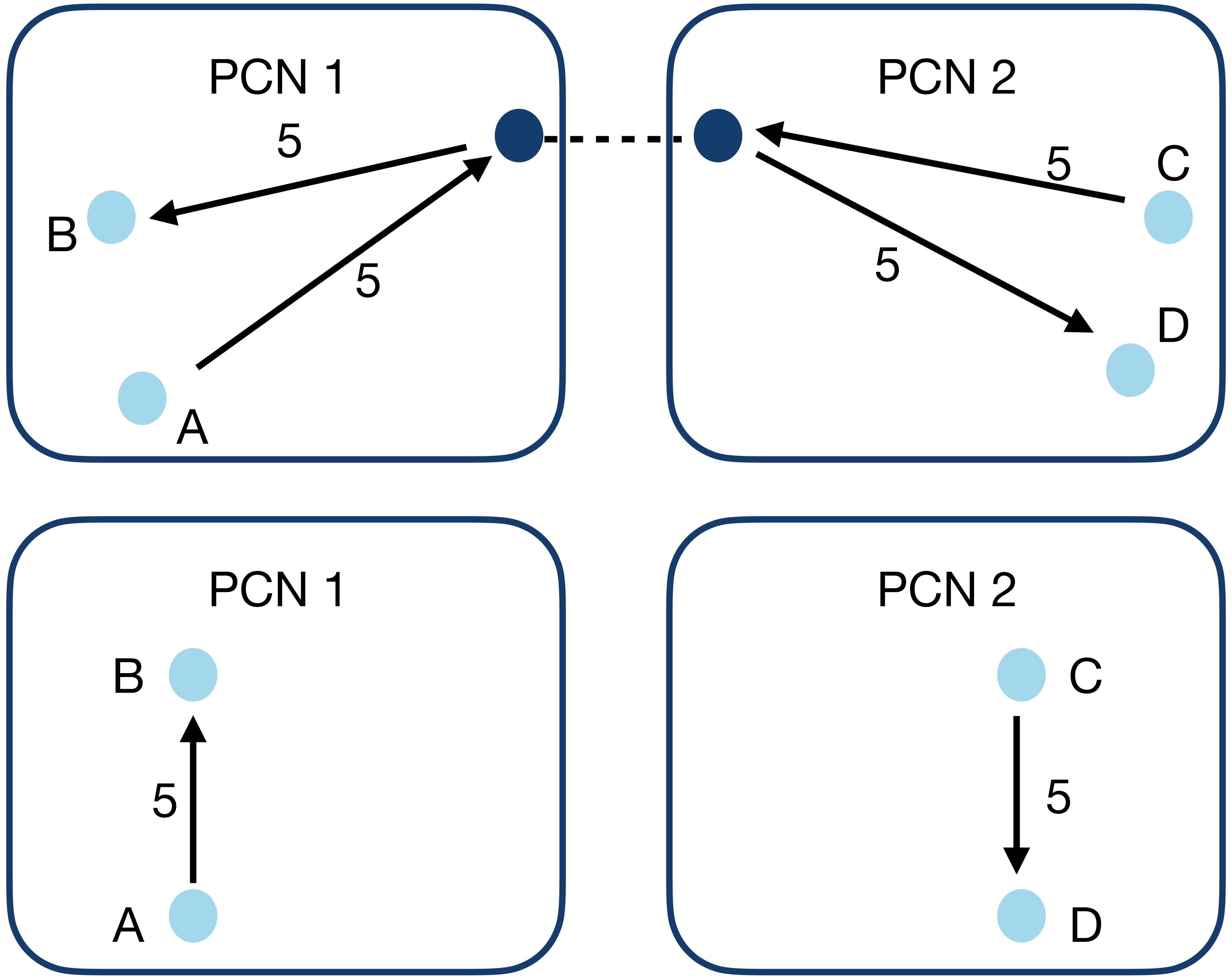
2. Security: what if intermediary runs away with payments?



Secure and interoperable PCNs

- Issues:

1. Interoperability: how to convert payments across two systems?
2. Security: what if intermediary runs away with payments?
3. Scalability: what if there are lots of payments?



Atomic cross-PCN transactions

Bridge solutions	[Herlihy18], [BKLZ20], [MTVFM23], [SAAMG23], [SABAM24]
TTP	[JYSLWL23]
Deposits	[ZQ23]

Atomic cross-PCN transactions

Bridge solutions	[Herlihy18], [BKLZ20], [MTVFM23], [SAAMG23], [SABAM24]
TTP	[JYSLWL23]
Deposits	[ZQ23]

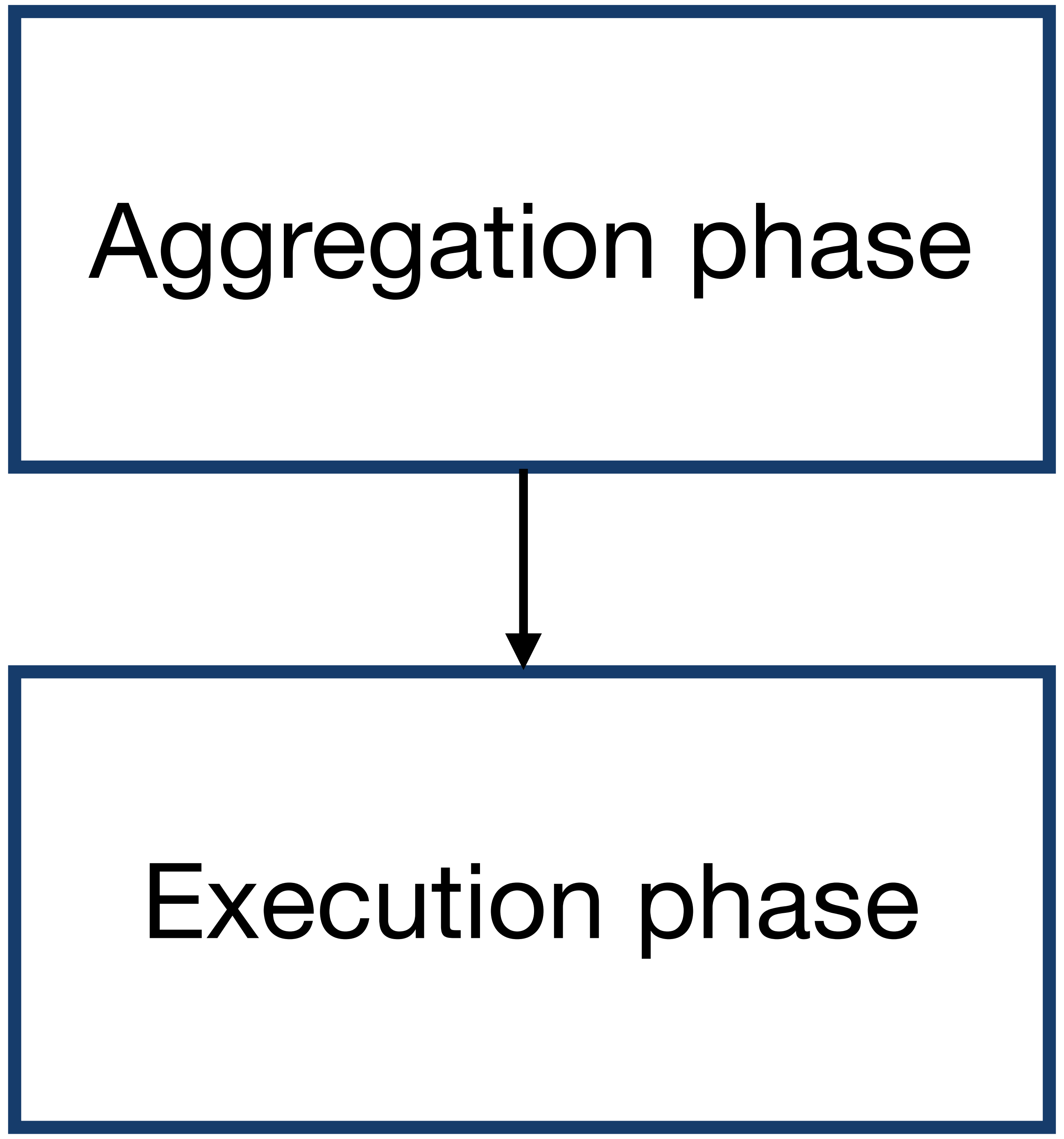
Our work: first lightweight, scalable, fully off-chain, non-TTP solution

X-transfer desiderata

- Balance security
- Fee minimisation
- Computational feasibility
- Privacy

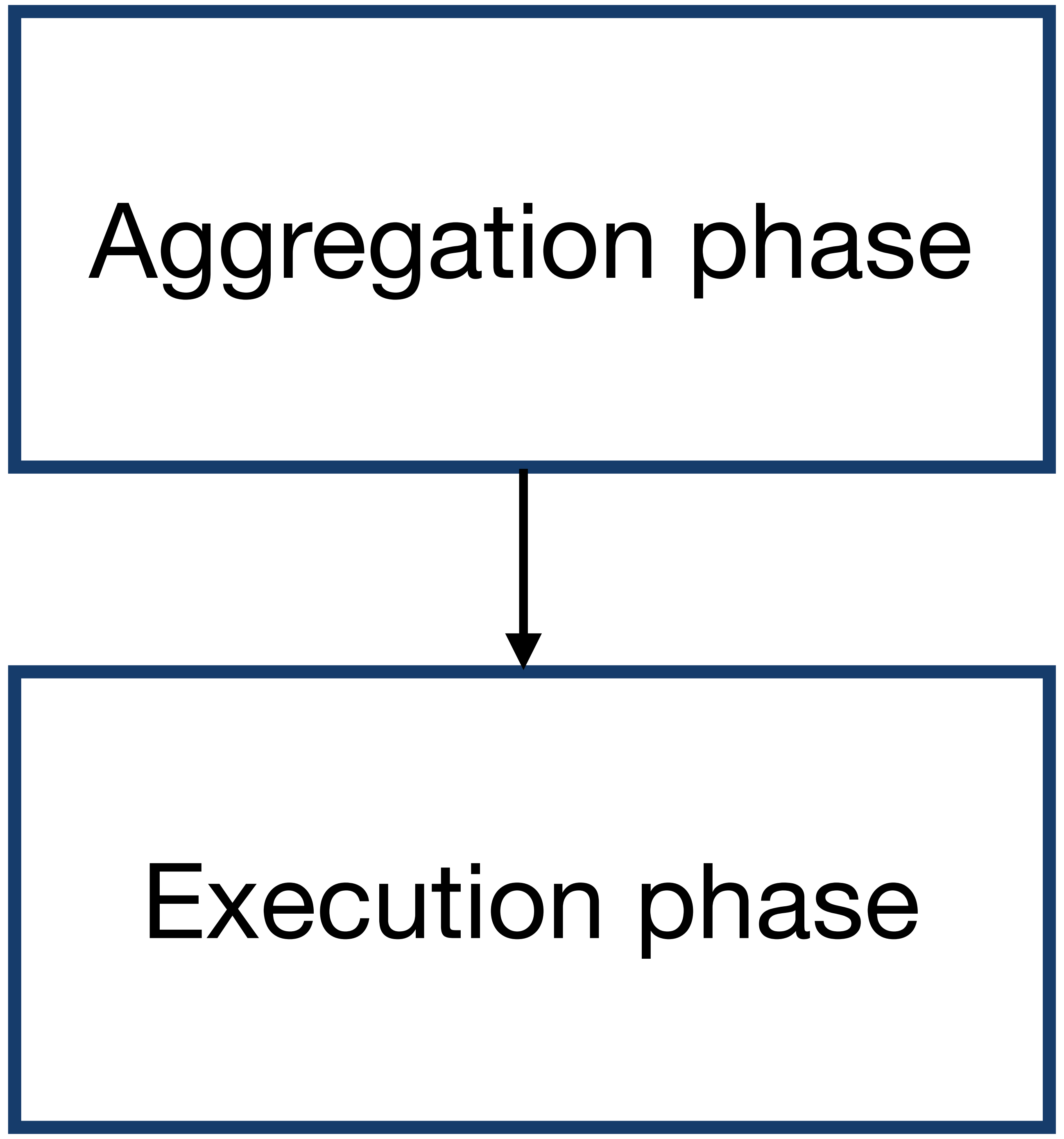
X-transfer

- Transaction aggregation + atomic cross-PCN execution



X-transfer

- Transaction aggregation + atomic cross-PCN execution
- Hub nodes: execute cross-PCN transfers
  - Hubs only execute transactions, do not send or receive
  - Star topology for efficient transaction aggregation[1]



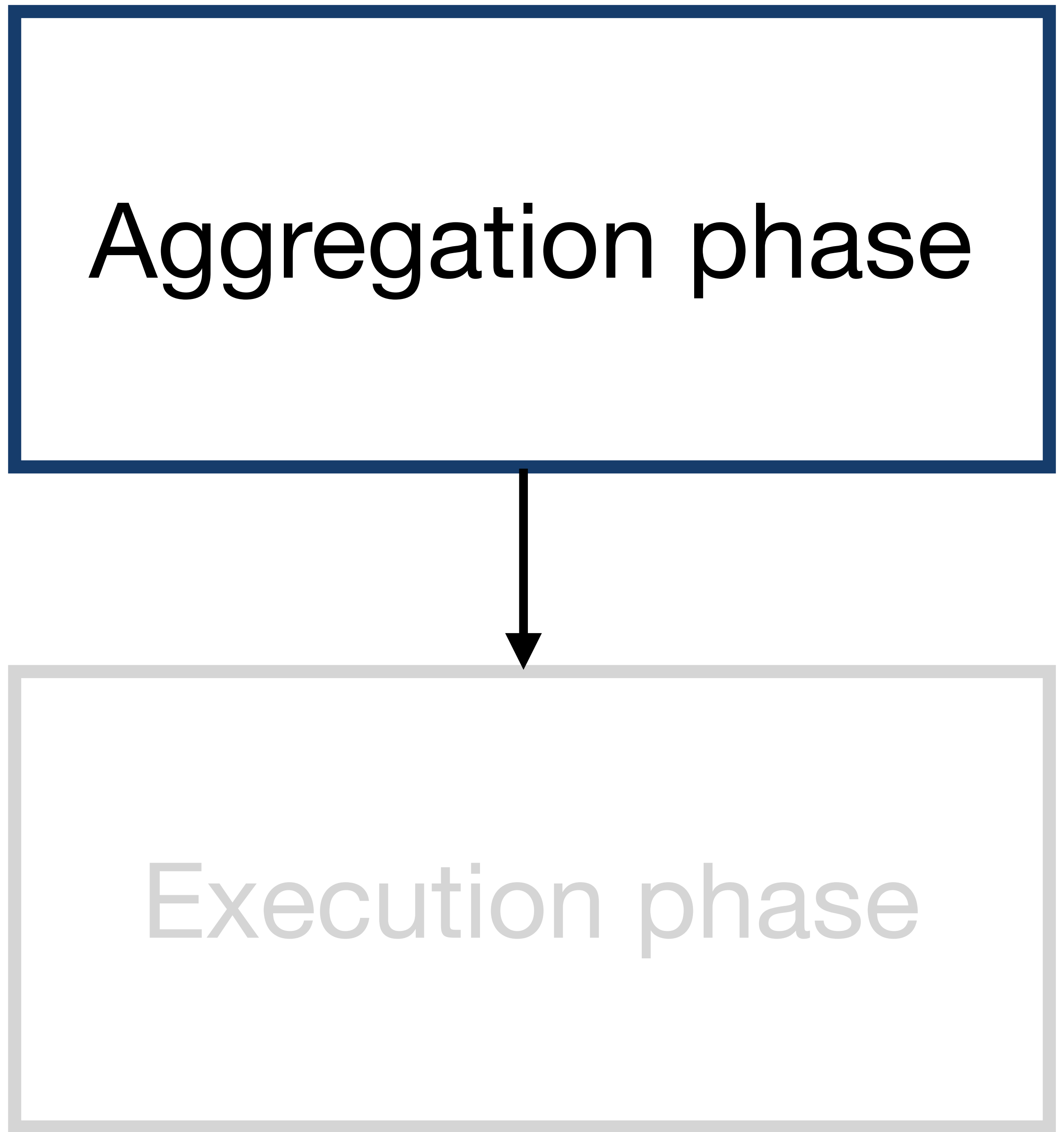
Aggregation phase

Execution phase

[1] Increasing Throughput in Payment Channel Networks with Transaction Aggregation. TYASPS. **AFT 2022**

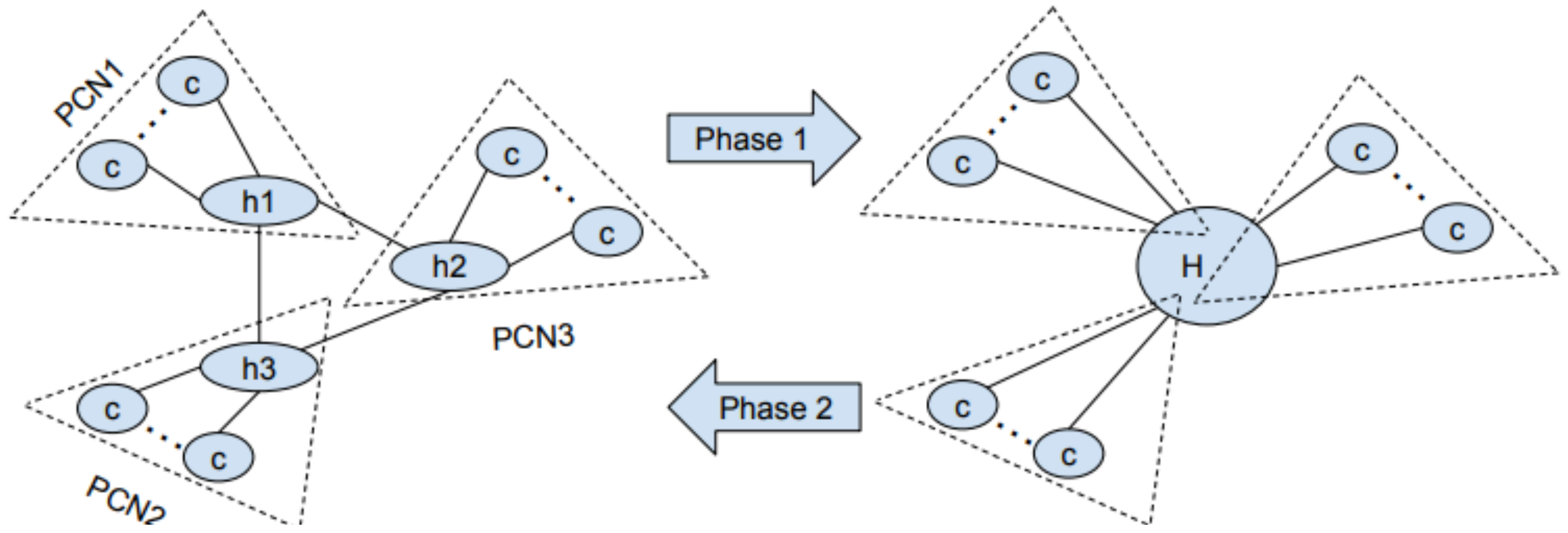
X-transfer: aggregation phase

- Goal:
  - Maximise client-to-hub transaction volume
  - Output optimal flow topology among hubs
  - Compute setup parameters for execution



X-transfer: aggregation phase

- Goal:
  - Maximise client-to-hub transaction volume →
  - Output optimal flow topology among hubs →
  - Compute setup parameters for execution



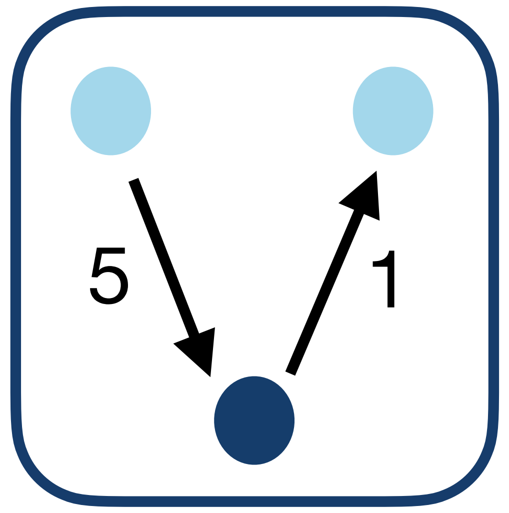
solve ILP and connect hubs

MPC to preserve privacy

X-transfer: aggregation phase

- Goal:
  - Maximise client-to-hub transaction volume
  - Output optimal flow topology among hubs
  - Compute setup parameters for execution →

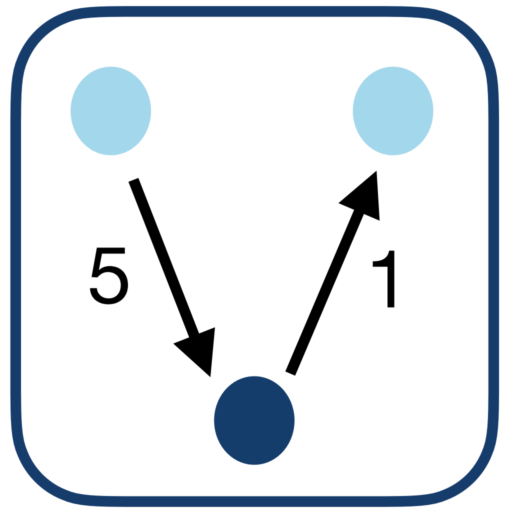
Safe PCNs: PCNs that have positive or 0 inflow from clients



X-transfer: aggregation phase

- Goal:
  - Maximise client-to-hub transaction volume
  - Output optimal flow topology among hubs
  - Compute setup parameters for execution →

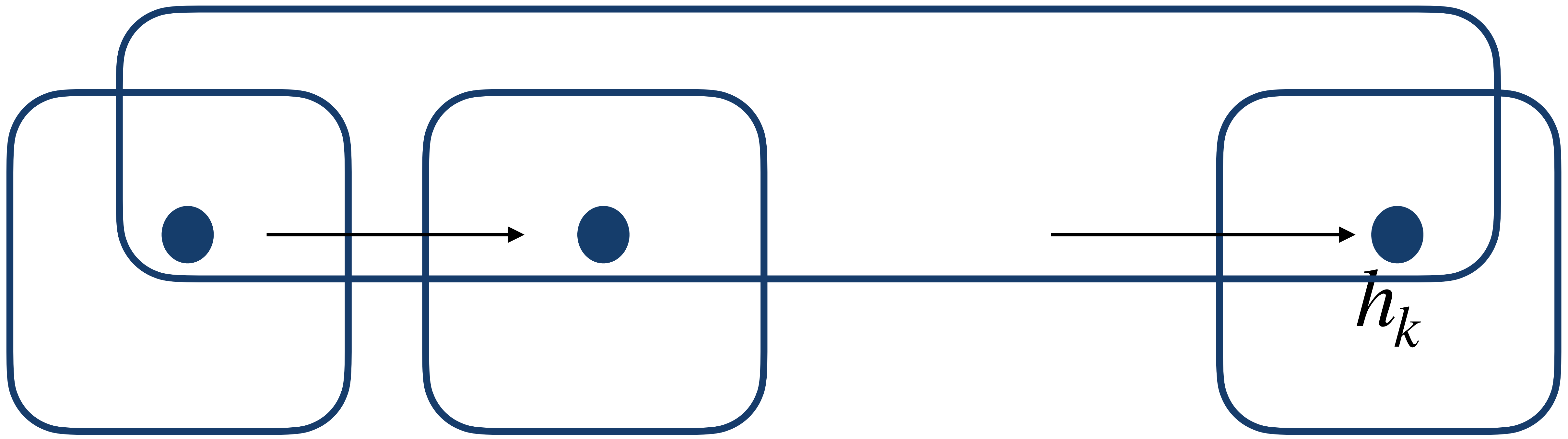
Safe PCNs: PCNs that have positive or 0 inflow from clients

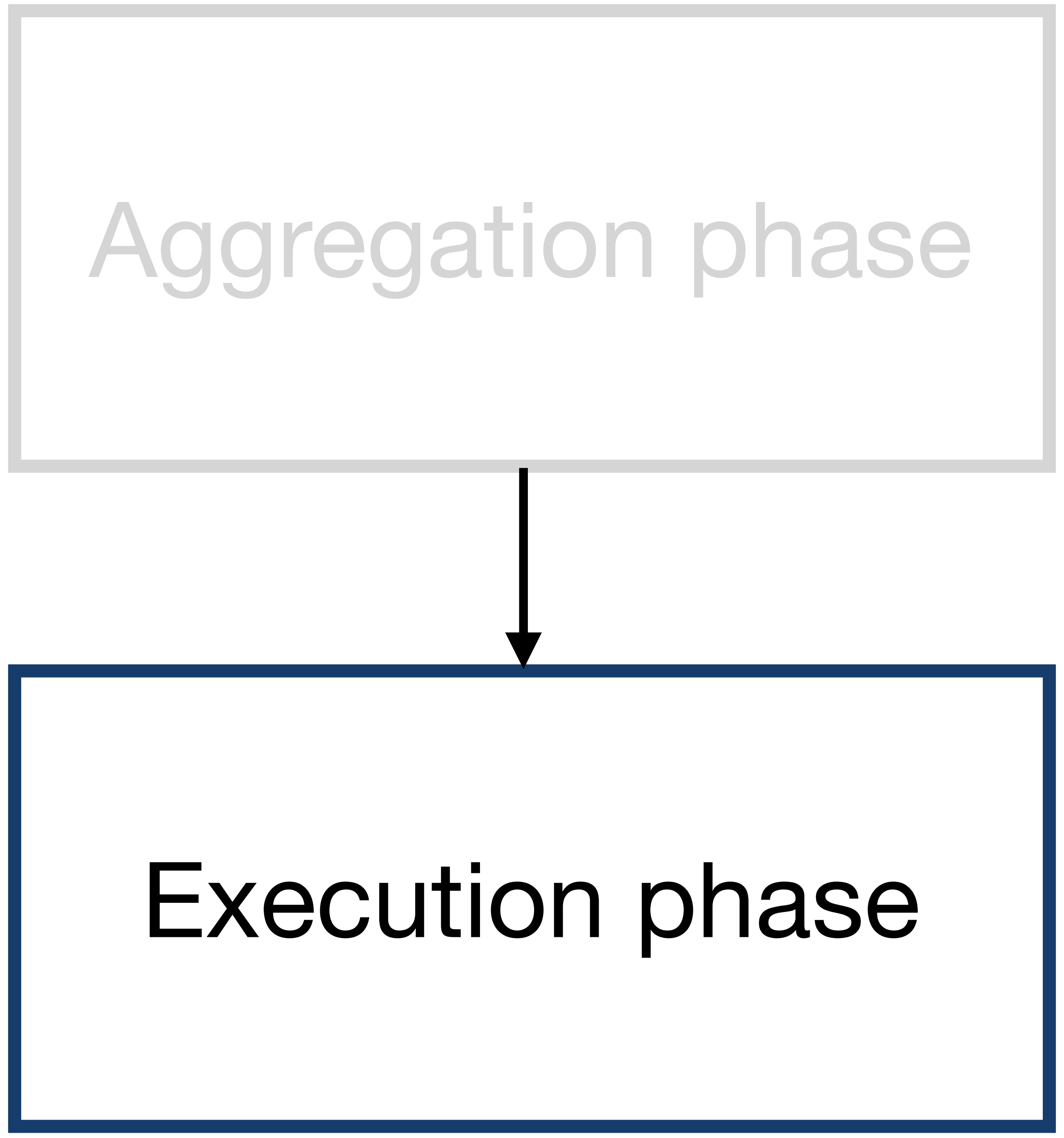


Invariants:

1. Safe PCNs execute first
2. There is a receiver in unsafe PCN that has a corresponding sender in a safe PCN

X-transfer: execution phase





- Thora[2] for atomic execution in each PCN

- h_k samples secret s, $H(s)$ additional hashlock

[2] Thora: Atomic and Privacy-Preserving Multi-Channel Updates. AAM. **CCS 2022**

X-transfer analysis

Theorem (informal)

X-transfer satisfies balance security, computational feasibility, near optimality and privacy

Conclusion

- X-transfer: first lightweight, scalable, fully off-chain cross-PCN transaction aggregation and payment protocol

- Future directions:

  - Fee structure for hubs

  - Exchange rates

michellexyeo@gmail.com